REMARKS

The August 27, 2004 Office Action has been reviewed and the claims have been amended in a fashion that is believed to place the application in condition for allowance.

In the Office Action, the Examiner rejected claims 1-3, 5, 9-10 under 35 USC § 103(a) as being obvious over Aziz (U.S. Patent No. 5,668,877) in view of Bell (U.S. Patent No. 6,707,914) in view of Dole (U.S. Patent No. 6,628,786) and further in view of Bellare (U.S. Patent No. 5,491,750). The Examiner objected to claims 4 and 6-8 as being dependent upon a rejected base claim, but as being otherwise allowable if rewritten in independent form including all base claim and intervening claim limitations. The Examiner has returned an initialed copy of Form PTO-1449 indicating consideration of the Applicants' Information Disclosure Statement.

The Examiner is thanked for noting allowable subject matter.

Claim 1 is amended to incorporate the subject matter of claim 2 and the features recited in allowable claim 4, subject to a change by deletion of "one of." (As a consequence of the incorporation of the subject matter of claims 2 and 4 into claim 1, those claims are cancelled without prejudice to the subject matter therein.)

More specifically, in the last paragraph of claim 4 that recites "the drop of information comprises a lost data on one of a sign data and a numeral data of a respective session key," the phrase "one of" is deleted in amended claim 1, to claim subject matter of the allowable claim 4, but also in consideration of new Information Disclosure Statement materials including:

5

Japanese Patent Application Laid-Open Publication No. 10-285154 (hereinafter "JP '154"), which has been cited as a reference during the prosecution of a corresponding national-phase application in the Japanese Patent Office; and

Japanese Patent Application Laid-Open Publication No. 10-20783 (hereinafter "JPA '783"), which has also been cited as a reference in the Japanese national phase application.

To provide a computationally secure entropy difference against crypto-analysis, the concept of one-directional thinning compression of a huge integer field generated by a chaotic mapping, as taught in JPA '783, employed a sequentially extended mapping. In JPA '154, results of such mapping were used as initial values for derived mappings to generate orbits of integers.

In contrast, the present invention is directed to a new concept, that is the "drop of information" recited in amended claim 1, which led the inventor to dropping s (s>0) digits, (*see* page 7, line 8 of the specification). As supported on pages 6-7 of the specification, the drop of information accompanies lost data not simply on sign data (+/-) but also on numerical data (s digits). The prior art is silent on this feature.

Remaining claims 3 and 5-10 now depend from the amended claim 1, and therefore should also be allowable.

As all grounds of objection and rejection have been addressed and overcome, entry of this Amendment and issuance of a Notice of Allowance of the claims, as now presented, are respectfully solicited.

In the event that there are any questions relating to this Amendment or to the application in general, it would be appreciated if the examiner would telephone the undersigned attorney concerning such questions so that the prosecution of this application may be expedited.

Please charge any shortage or credit any overpayment of fees to BLANK ROME LLP, Deposit Account No. 23-2185 (000004-00662). In the event that a petition for an extension of time is required to be submitted herewith and in the event that a separate petition does not accompany this response, Applicants hereby petition under 37 C.F.R. 1.136(a) for an extension of time for as many months as are required to render this submission timely.

Any fees due are authorized above.

Respectfully submitted,

EIJI WATANABE et al.

By: Michael D. White
Reg. No. 32,795

BLANK ROME LLP
WATERGATE
600 NEW HAMPSHIRE AVENUE, NW
WASHINGTON, DC 20037
PHONE: (202) 772-5800
FAX: (202) 572-8398